REMARKS

1. Introduction

In the Office Action mailed July 30, 2010, the Examiner rejected claims 1-18, 21-25, 28-45, and 48-88 under 35 U.S.C. § 103(a) as being unpatentable over Hashimoto et al., U.S. Pub. No. 2002/0053024 ("Hashimoto") in view of Nguyen et al., U.S. Pub. No. 2002/0116615 ("Nguyen") and Borgelt et al., U.S. Patent No. 5,398,285 ("Borgelt").

The Examiner rejected claims 19-20, 26-27, and 46-47 under 35 U.S.C. § 103(a) as being unpatentable over Hashimoto, Nguyen, and Borgelt in view of Reeder, U.S. Patent No. 6,141,652 ("Reeder").

The Examiner also rejected claims 18-23, 44-51, and 76-88 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

In response, Applicant has amended claims 16, 17, 44, 76, and 80.

For the reasons set forth below, Applicant requests reconsideration and allowance of the application, as amended herein.

2. Response to the claim rejections under § 101

The Examiner has rejected claims 18-23, 44-51, and 76-88 under 35 U.S.C. § 101 as being directed to non-statutory subject matter, arguing that "these are method or process claims that do not transform underying subject matter (such as an article or materials) to a different state or thing, nor are they tied to another statutory class (such as a particular machine)." *See* Office Action, p. 2. In this regard, the Examiner has taken the position that method claims must pass the "machine-or-transformation test" in order to be eligible under § 101.

Applicant submits that the Examiner's position is incorrect in view of the Supreme Court's recent decision in *Bilski v. Kappos*. Nonetheless, in order to expedite prosecution, Applicant has amended the independent method claims as follows:

- Applicant has amended claim 16 to recite "configuring the processor module," thereby reciting a transformation of an article to a different state;
- Applicant has amended claim 44 to recite "a security module" performing the step of "decrypting the downloaded encrypted software program" and then either enabling or disabling execution of the downloaded encrypted software program, thereby tying the method to a particular machine; and
- Applicant has amended claim 76 to recite "configuring the processor module," thereby reciting a transformation of an article to a different state.

As a result, the method claims in the application (claims 16-23, 44-51, and 76-88) pass the "machine-or-transformation test" and are clearly statutory. Accordingly, Applicant respectfully requests that the rejections of claims 18-23, 44-51, and 76-88 under § 101 be withdrawn.

3. Response to the claim rejections under § 103

Of the currently pending claims, claims 1, 16, 24, 44, 52, and 76 are independent. The Examiner has rejected each of these independent claims under § 103 as being unpatentable over Hashimoto in view of Nguyen and Borgelt. In response, Applicant submits that this rejection is improper and should be withdrawn because the Examiner has not set forth a valid rationale for why a person of ordinary skill in the art would have combined the teachings of Borgelt with the teachings of Hashimoto.

Claim 1 recites, *inter alia*, "a security module ... arranged to decrypt an encrypted software program to recover an identification code therefrom, to enable execution of the software program by the processor ... when the recovered identification code matches the unique identification code associated with the processor module, and to disable execution of the software program when the identification code does not match the unique identification code associated with the processor module." The other independent claims also recite functions relating to enabling or disabling execution depending on whether a recovered or decrypted identification code matches a unique identification code, as summarized below:

- Claim 16 recites, *inter alia*, "configuring the processor module to enable execution of the encrypted software program by the processor module when the decrypted identified code is the same as the unique identification code of the processor module and configuring the processor module to disable execution of the encrypted software program by the processor module when the decrypted identification code is different from the unique identification code of the processor module";
- Claim 24 recites, *inter alia*, "a security module ... enabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is the same as the unique identification code of the particular player station, and disabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is different from the unique identification code of the particular player station";
- Claim 44 recites, *inter alia*, a "security module enabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is the same as the unique identification code of the particular player

station, and the security module disabling execution of the downloaded encrypted software program by the particular player station when the decrypted identification code is different from the unique identification code of the particular player station";

- Claim 52 recites, inter alia, "a security module ... enabling execution of the downloaded encrypted software program by the particular processor module when the decrypted identification code is the same as the unique identification code of the particular processor module, and disabling execution of the downloaded encrypted software program by the particular processor module when the decrypted identification code is different from the unique identification code of the particular processor module"; and
- Claim 76 recites, *inter alia*, "configuring the processor module to enable execution of the downloaded encrypted software program by the particular processor module when the decrypted identified code is the same as the unique identification code of the particular processor module, and configuring the processor module to disable execution of the downloaded encrypted software program by the particular processor module when the decrypted identification code is different from the unique identification code of the particular processor module."

In rejecting claim 1 and the other independent claims, the Examiner admitted that Hashimoto does not teach "recovering a unique identification code from the encrypted software program and only executing the game when the recovered code matches the unique identification code associated with the processor module." *See* Office Action, p. 4 (claim 1), p. 8 (claim 16), p. 12 (claim 24), p. 18 (claim 44), p. 22 (claim 52), and p. 30 (claim 76). Instead, the Examiner relied on Borgelt, arguing that "Borgelt teaches a system in which a unique identification code associated with a first system is sent to a software distributor, encrypted in a return message with

a software code, decrypted by a receiving first system, and confirming that the unique identifier received matches the unique identifier of the system before executing the program using the software code." *See* Office Action, p. 4 (claim1), p. 8 (claim 16), pp. 12-13 (claim 24), p. 18 (claim 44), pp. 22-23 (claim 52), and p. 30 (claim 76). According to the Examiner, a person of ordinary skill in the art would have modified Hashimoto to include the steps of Borgelt to "insure that even in the case where the software ... is decrypted using another machine's identifier the receiving machine will still not execute the software unless the identifier matches the receiving machine." *See* Office Action, p. 5 (claim1), p. 9 (claim 16), p. 13 (claim 24), p. 19 (claim 44), p. 23 (claim 52), and p. 31 (claim 76).

The flaw in the Examiner's argument is that the problem supposedly solved by Borgelt's approach would not actually occur in Hashimoto's method. In particular, "another machine's identifier" would not be able to decrypt the software that is distributed in Hashimoto's method. As described in paragraph 23 of Hashimoto, the execution file is decrypted using "a secret key corresponding to the public key" and the "public key ... is either unique to the execution file receiving device or unique to a processor of the execution file receiving device." This means that the secret key corresponding to the public key is also unique to the execution file receiving device or its processor. As a result, the secret key of a different receiving device, what the Examiner described as "another machine's identifier," would not be able to decrypt the execution file in Hashimoto. Because the alleged problem which is the premise for the Examiner's rationale for combining Borgelt with Hashimoto is not a realistic problem, the Examiner's rationale is necessarily invalid.

The Examiner also referred to the problem described in Borgelt at col. 1, line 60 – col. 2, line 11. But the problem described in that section is also not a problem that would be

encountered in Hashimoto's method. The basic problem described in Borgelt is that a password which can enable premium features of a communication device is already present in the communication device, albeit in an encrypted form. As a result, if the encryption/decryption scheme is discovered, the password could be recovered and the premium features could be enabled without authorization. In contrast, no such vulnerable password is present in Hashimoto's method. Moreover, the communication device in Borgelt is particularly vulnerable because the software that is capable of providing the premium features is also already present in the device. Thus, the correct password is all that is needed to enable the premium features. *See* col. 1, lines 25-59. In contrast, in Hashimoto's method, the software is distributed to a device in an encrypted form rather then being loaded in the device in advance.

In summary, Hashimoto's method already ensured that the execution file is executed by only the intended receiving device, in that the execution file is decrypted by a secret key that is unique to the intended receiving device. Therefore, a person of ordinary skill in the art would have had no reason to use a unique identification code as described in Borgelt.

Accordingly, Applicant submits that claims 1, 16, 24, 44, 52, and 76 are allowable over Hashimoto in view of Nguyen and Borgelt for at least the foregoing reasons. Applicant further submits that claims 2-15, 17-23, 25-43, 45-51, 53-75, and 77-88 are allowable for at least the reason that they depend from allowable claims.

4. Conclusion

Applicant submits that the present application is in condition for allowance, and notice to that effect is hereby requested. Should the Examiner feel that further dialog would advance the

subject application to issuance, the Examiner is invited to telephone the undersigned at any time at (312) 913-0001.

Respectfully submitted,

Date: September 29, 2010

By: Richard A. Machonkin

Richard A. Machonkin
Registration No. 41,962

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001